

Melihat Lalu Lintas di Network Dengan NTOP

Tom Gregory

tom@security-1st.net

http://tom149c.blogspot.com

Lisensi Dokumen:

Copyright © 2003 IlmuKomputer.Com

*Seluruh dokumen di **IlmuKomputer.Com** dapat digunakan, dimodifikasi dan disebarluaskan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari **IlmuKomputer.Com**.*

NTOP adalah tool untuk melihat traffic di network dan menampilkannya untuk kita dalam bentuk yang luar biasa hebat. NTOP sendiri diklaim sebagai tool network probing open source paling handal, setidaknya menurut saya :). Berbeda dengan program sejenis seperti cacti, MRTG, nagios, dan lainnya, NTOP lebih tenang dalam penyajian tampilan dan relatif enak dilihat tanpa opsi-opsi dan pilihan-pilihan fitur yang rumit. NTOP melakukan probing hampir sama dengan program top pada linux sehingga admin dapat melihat aktifitas network dengan mudahnya. Hebatnya lagi, tampilannya disajikan secara web based dan enak dilihat.

Komputer server tempat NTOP berdiam memiliki spesifikasi sebagai berikut :

System Operasi	:	Slackware 11.0
Prosesor sistem	:	Pentium III 733 Mhz
Memori	:	311 MB
HDD	:	20 GB

Tahap Pertama

Download program Ntop disitusnya :

```
$ pwd  
/home/t0m  
$ wget http://optusnet.d1.sourceforge.net/sourceforge/ntop/ntop-3.3rc1.tgz
```

Tahap Kedua

Ekstrak file ntop yang telah di download :
(jadi root dulu)

```
$ su  
Password :  
#  
# tar xzvf ntop-3.3rc1.tgz -C /usr/src/ntop/
```

Dependensi Program NTOP :

Program RRDTool

NTOP membutuhkan program RRDTool untuk menampilkan dalam grafik, jadi kita musti download dulu program RRDTool.

```
# wget http://ftp.naist.jp/pub/Linux/linuxpackages/Slackware-11.0/Console/RRDtool/rrdtool-1.2.19-i486-2gds.tgz
```

Setelah itu, lakukan instalasi sebagai berikut:

```
# installpkg rrdtool-1.2.19-i486-2gds.tgz
```

Program LIBPCAP

Program LIBPCAP digunakan NTOP untuk mengcapture paket-paket data yang lewat di network.

```
# wget http://www.tcpdump.org/release/libpcap-0.9.5.tar.gz
```

Lakukan instalasi sebagai berikut :

```
# tar xzvf libpcap-0.9.5.tar.gz -c /usr/src/  
# cd /usr/src/libpcap-0.9.5  
# ./configure && make && make install
```

Beres..tapi untuk mempercantik hasil dari keluaran NTOP, ada satu program optional lagi, namanya graphviz. Saya sih tidak mengharuskan, tapi program ini benar-benar menambah kehebatan si NTOP :)

Program Graphviz

download graphviz :

```
# wget http://www.graphviz.org/pub/graphviz/ARCHIVE/graphviz-2.12.tar.gz
```

Lakukan instalasi sebagai berikut :

```
# tar xzvf graphviz-2.12.tar.gz -c /usr/src/  
# cd /usr/src/graphviz-2.12/  
# ./configure && make && make install
```

Kalo ada error, berarti kebutuhan dependensi graphviz belum lengkap, silakan baca-baca kebutuhannya di http://www.graphviz.org/Download_source.php. Cara instalasinya sama dengan diatas.

Tahap Ketiga

Instalasi program NTOP :

```
# cd /usr/src/ntop-3.3rc1/  
# ./autogen.sh  
# make  
# make install
```

Tahap Keempat

Saya biasa membuat user khusus untuk ntop dengan alasan keamanan, apabila terjadi hal-hal diluar dugaan pada program tersebut, user ntop-lah yang terkena akibatnya bukan satu sistem atau user lain.

Membuat user NTOP

```
# groupadd ntop
# useradd -g ntop -s /sbin/nologin -d /usr/local/var/ntop -c "##### ntop" ntop
```

Menjalankan program NTOP:

Pertama-tama ntop akan meminta password untuk admin, silakan jalankan ntop dengan perintah:

```
# /usr/local/bin/ntop
```

Lalu jalankan program NTOP sebagai serveice dengan perintah-perintah sebagai berikut :

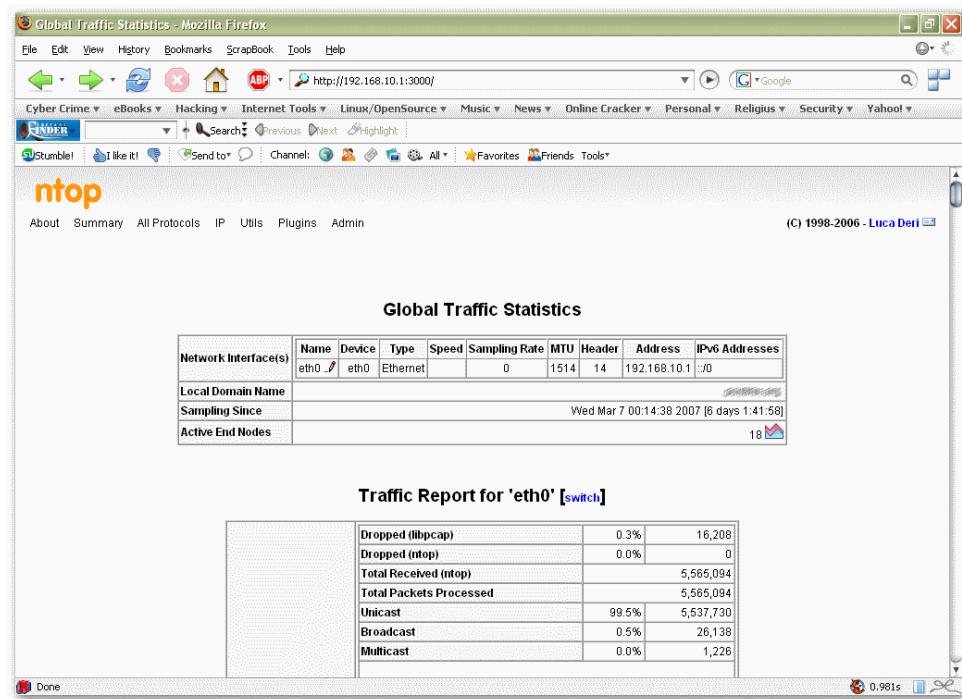
```
# ./usr/local/bin/ntop -u ntop -i [interface network yg mau dimonitor] -d -w
[default port adalah 3000]
```

Silakan mengecek apakah program NTOP benar-benar berjalan :

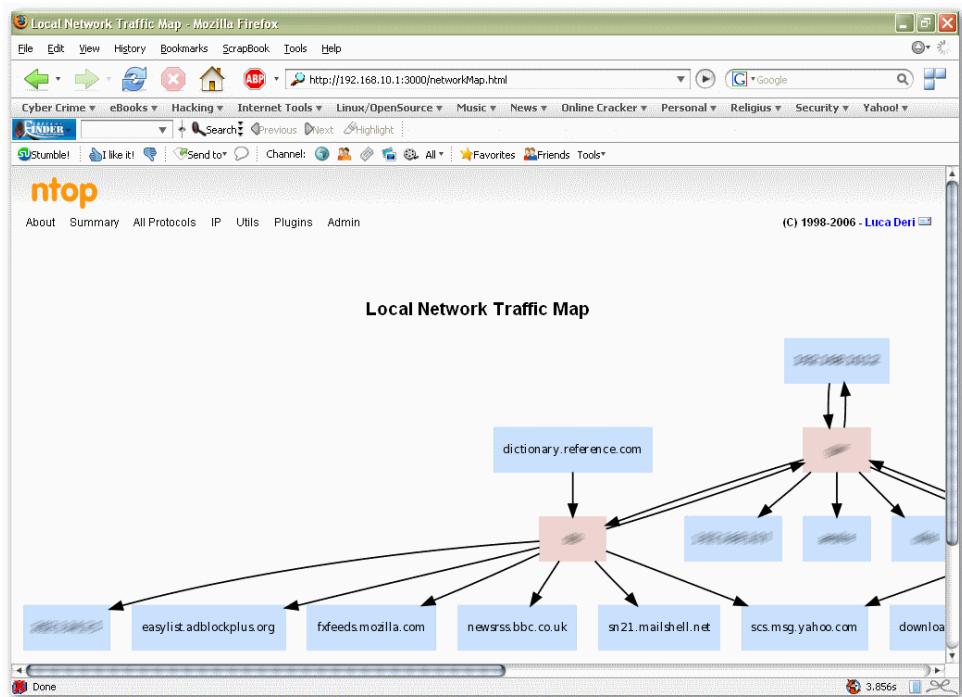
```
# ps ax | grep ntop
2566 ?      ss1    27:00 /usr/local/bin/ntop -u ntop -i eth0 -d -w 3000
16563 pts/2   R+     0:00 grep ntop
#
```

Yup, sukses berjalan. Sekarang kita bisa browse untuk melihatnya, silakan pergi ke browser kesayangan Anda dan arahkan ke IP Address tempat menginstall NTOP, misal <http://192.168.10.1:3000>

Seharusnya akan tampil seperti ini :



Dan kelebihan yang saya bicarakan itu adalah :)



Semuanya sangat jelas terlihat mulai dari mana dan kemana saja klien kita berselancar :)

Sampai disini, NTOP sudah berjalan dengan lancar, dan agar dapat berjalan lagi ketika komputer di restart (baca: autostart), maka kita perlu meng-edit file rc.local :

```
# pico /etc/rc.d/rc.local
```

Masukkan baris berikut :

```
/usr/local/bin/ntop -u ntop -i eth0 -d -w 3000
```

Simpan filenya, dan booting komputer kalau tidak percaya :)

Selesai sudah tahap-tahap instalasi program NTOP.

Biografi Penulis



Thomas Gregory Ajawaila. Lahir di Jakarta, 28 Mei 1984. Selesai menamatkan Sekolah Menengah Umum Marsudirini Bekasi tahun 2002. Masih berjuang untuk menyelesaikan kuliah di STIMIK Perbanas Jakarta angkatan 2002. Saat ini sedang mendalami ilmu keamanan komputer dan melakukan riset terhadap perkembangan keamanan komputer melalui jaringan RT/RW Net. Aktif dalam organisasi kampus sebagai pencetus dan pendiri Himpunan Mahasiswa Sistem Informasi STIMIK Perbanas merangkap ketua pada periode 2006/2007. Penulis juga berlaku sebagai Moderator pada mailing list Jasakom (http://groups.yahoo.com/group/jasakom_perjuangan) dan sebagai Owner pada mailing list Jasakom-Moderator (<http://groups.yahoo.com/group/jasakom-moderator>). Penulis aktif di komunitas Jasakom dan melakukan riset serta penelitian, kecenderungan untuk menulis pun tak bisa dihindari.

Berpengalaman sebagai system administrator pada web server STIMIK Perbanas (<http://stibanas.ac.id>), sebagai hacking trainer pada beberapa instansi / lembaga training seperti Informatics, dan Sokka Data Informatika yang telah melayani klien-klien dari beberapa perusahaan dan instansi pemerintah seperti PT. Wijaya Karya, Pusintek Departemen Keuangan, TNI-AL, dan PT. Sinar Mas.

Informasi lebih lanjut tentang penulis ini bisa didapat melalui:

URL : <http://tom149c.blogspot.com>
Email : t0m@stibanas.ac.id / tom@security-1st.net